Innovative approach for resolving Sybil Attack in MANET

Vivek Jaglan

Assistant professor, Dept. of CSE, Amity University Gurgaon

Abstract— **Wireless ad hoc networking is a technology that allows fast, easy, and inexpensive network deployment. Unfortunately, these advantages also make the task of an attacker simpler, as it is also easier to deploy a malicious node in the environment.. A number of schemes have been proposed, but they differ greatly in the algorithms they use and in the networks upon which they are evaluated. As a result, the research community lacks a clear understanding of how these schemes compare against each other, how well they would work on real-world social networks with different structural properties, or whether there exist other (potentially efficient) ways of Sybil defence. In this paper, we present a technique through which Sybil attack can be removed effectively as compared to existing techniques. By this method, there is reduced packet loss, throughput, jitter compared to the existing or classical approach of Sybil attacks. We show through simulation that Sybil attack can be prevented by proposed solution. Finally, we identify areas where further research could focus.**

Keywords— **MANET, Network Security, Attacks.**

I. Introduction

A mobile ad hoc network is a collection of wireless nodes that can dynamically be set up anywhere and anytime without using any pre-existing network infrastructure. It is an autonomous system in which mobile hosts connected by wireless links are free to move randomly. In MANET, nodes act both as host and routers. The traffic types in ad hoc networks are quite different from those in an infrastructure wireless network, including:

1. Peer-to-Peer: Communication between two nodes, which are within one hop.
2. Remote-to-Remote: Communication between two nodes beyond a single hop but which maintain a stable route between them. This may be the result of several nodes staying within communication range of each other in a single area or possibly moving as a group. The traffic is similar to standard network traffic.
3. Dynamic Traffic: This occurs when nodes are dynamic and moving around. Routes must be reconstructed. This results in a poor connectivity and network activity in short bursts.

II. MANET Vulnerabilities

1. Lack of centralized management: MANET doesn't have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale ad-hoc network. Lack of centralized management will impede trust management for nodes.
2. Resource availability: Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.
3. Scalability: Due to mobility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.
4. Cooperativeness: Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.
5. Dynamic topology: Dynamic topology and changeable nodes membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised. This dynamic behaviour could be better protected with distributed and adaptive security mechanisms.
6. Limited power supply: The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems. A node in mobile ad-hoc network may behave in a selfish manner when it is finding that there is only limited power supply.
7. Bandwidth constraint: Variable low capacity links exists as compared to wireless network which are more susceptible to external noise, interference and signal attenuation effects.
8. Adversary inside the Network: The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously. This is hard to detect that the behaviour of the node is malicious. Thus this attack is more dangerous than the external attack. These nodes are called compromised nodes.
9. No predefined Boundary: In mobile ad- hoc networks we cannot precisely define a physical boundary of the network. The nodes work in a nomadic environment where they are allowed to join and leave the wireless network. As soon as an adversary comes in the radio range of a node it will be able to communicate with that node. The attacks include Eavesdropping impersonation; tempering, replay and Denial of Service (DoS) attack [2].

III. MANET Challenges

The features of MANET introduce several challenges that must be studied carefully before a wide commercial deployment can be expected. These include:

1. Limited bandwidth: Wireless link continue to have significantly lower capacity than infrastructure networks. In addition, the realized throughput of wireless communication after accounting for the effect of multiple access, fading, noise, and interference conditions, etc., is often much less than a radio's maximum transmission rate.

2. Dynamic topology: Dynamic topology membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised.

3. Routing Overhead: In wireless adhoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.

4. Hidden terminal problem: The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver.

5. Packet losses due to transmission errors: Ad hoc wireless networks experiences a much higher packet loss due to factors such as increased collisions due to the presence of hidden terminals, presence of interference, uni directional links, frequent path breaks due to mobility of nodes.

6) Mobility-induced route changes: The network topology in an ad hoc wireless network is highly dynamic due to the movement of nodes; hence an on-going session suffers frequent path breaks. This situation often leads to frequent route changes.

7. Battery constraints: Devices used in these networks have restrictions on the power source in order to maintain portability, size and weight of the device.

8. Security threats: The wireless mobile ad hoc nature of MANETs brings new security challenges to the network design. As the wireless medium is vulnerable to eavesdropping and ad hoc network functionality is established through node cooperation, mobile ad hoc networks are intrinsically exposed to numerous security attacks.

IV. The Sybil Attack

Malicious nodes in a network may not only impersonate one node, they could take up the identity of a group of nodes, and this attack is called the Sybil attack. Since ad hoc networks depend on the communication between nodes, many systems apply redundant algorithms to ensure that the data gets from point A to point B. A consequence of this is that attackers have harder time to destroy the integrity of information. However, if a single malicious node is able to represent several other nodes, the effectiveness of these measures is significantly degraded. The attacker may get access to all the data or may alter all packets in the same transmission so that the destination node/s cannot detect the change in packets anymore. In trust-based routing environments, representing multiple identities can be used to deliver fake recommendations about the trustworthiness of a certain party, hereby attracting more traffic to it; in ideal starting point for further attacks. Amplified if the malicious node exists within or around the centre of the network so that it hears every communication happening inside the network. However, in the case of Multipath protocols which send data redundantly, not relying on one path only, the problem of sinkholes can be reduced.

Figure 1- Sybil Attack

Existing of Sybil Attack

In existing technique they followed RSS (Received Signal Strength), so if any nodes with RSS greater than the given threshold will be considered as the attacker. This approach is totally not applicable for the MANET because mobile nodes may have various signal strength.

In existing system, any node can act as the source and destination node. The destination node receive information from any node either it is actual or fake node (hacker's node) thereby leads to lack of accountability of the network.

V. Proposed Solution

This work centre particularly on discovery and shirking of Sybil assaults on the system base whether it is concerned with the sniffing of bundles or taking the genuine distinguish of the bona fide hub. This technique prevents the malicious node from attacking other nodes

Step 1

The remote hubs helping or taking an interest in the system to get to administration like web registers its character with the server executor, the server operator answers with special ID to the asking for hub.

Step 2

The source node attempts the request route with current access point for the destination wireless node and in this way the current access point forwards the route request to the server agent.

Step 3

The server agent verifies the source ID, then it accepts the route request from sender then it gathers the information of receiver using destination ID from the list.

Step 4

The server operator then telecasts the course ask for message utilizing terminus ID, the enrolled nearby hubs that are closer to the goal hub which are primed to give the administration answers the acknowledgement message to the server executor.

Step 5

The server agent chooses the adjacent node with the longest life time (the ability of the nodes to stay connected with the destination node) using the details collected from the ID, Such as nodes position, direction of motion and speed of the node.

Step 6

Then the server agent provides route reply message for the source node, after this authentication process, source node starts sending data packets in a secure way.

Step 7

The movement of source node and destination is monitored by another two nodes.

Step 8

Each node is controlled and connected by a cluster head and the data is sent to destination through cluster head.

Step 9

In case any node moves away from the network, immediately the server agent replaces it with some other nodes to maintain the continuity of connection.

Step 10

In this technique, the malicious node or selfish nodes are completely eliminated from the network, as the server agent takes full control of the ad-hoc network.

The proposed solution is implemented using the NS2 simulator. The first and second figures show the comparison of packet loss in the existing solution and proposed solution. The Second figure shows the average end to end delay analysis. The fourth figure shows the throughput analysis of proposed approach.

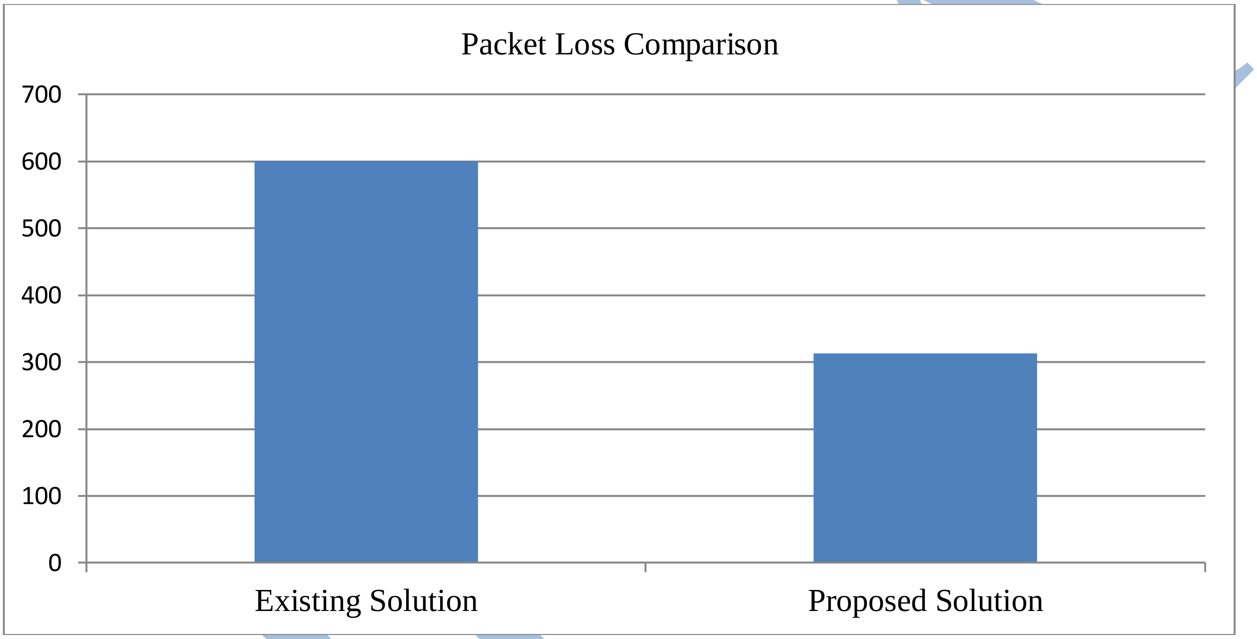

Figure 2– Packet Loss Parameter Analysis

The above figure shows that the existing solution contains 600 packet loss but the proposed solution drops only 313 packets. Hence, the proposed solution reduces packet loss up to 50% as compared with the existing approach.

The result validation is done by the journal named "Effective algorithm for reduces packet loss in Sybil attacks [10] which reduces the packet loss from 600 to 520.

Average Packets End to End Delay

Average End to End Delay means average time taken by a data packet to arrive in the destination. Its lower value leads to better performance.

Average end to end delay = ∑ (arrive time – sent time) / no. of connections

The graph below shows the average end to end delay for packet transferring between

- node E(intermediate node between source and cluster head 2) to CH2
- CH2 to server agent
- Server agent to CH1
- CH1 to destination node

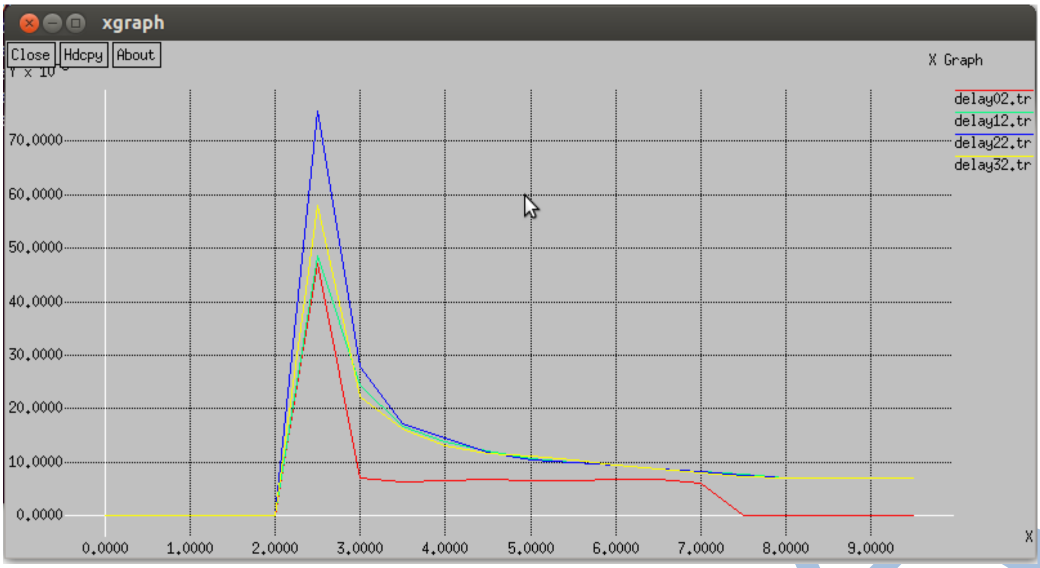

Figure-3– Average End to End Delay Analysis

The graph shows that there is an increase in end to end delay at simulation time from 2sec to 3sec and then decreases after 3 sec and remains almost constant after that throughout simulation. This shows that end to end delay gradually increases when communication starts but lows down after 3 sec during the communication.

VI. Throughput Analysis

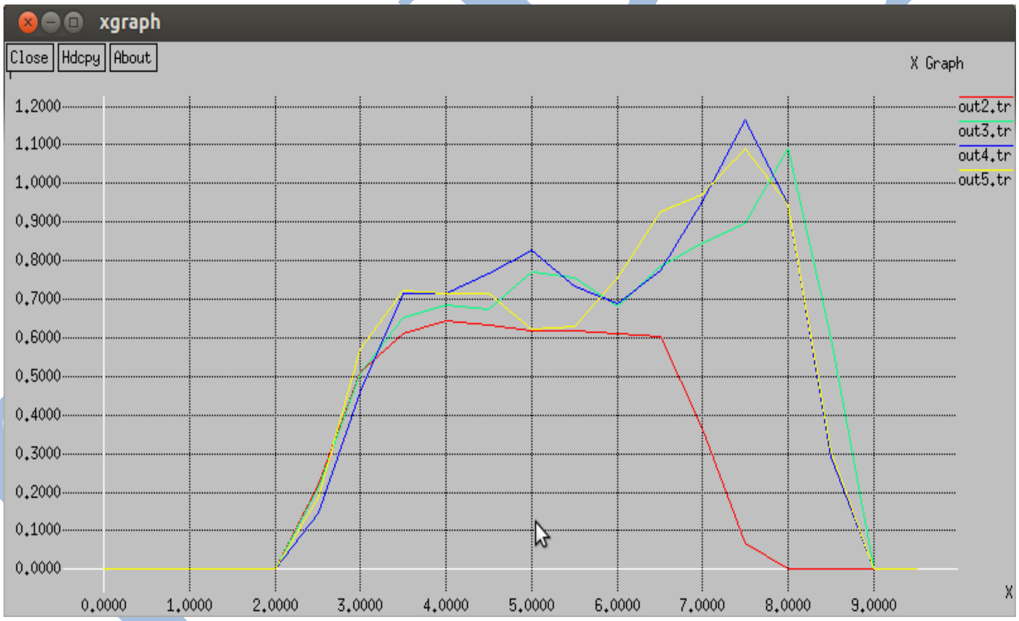

Figure-4– Throughput Analysis

Throughput means the amount of data transferred from source to destination or processed in a specified amount of time. Maximum data throughput leads to better network performance. The graph above shows the throughput for packet transferring between:

- node E(intermediate node between source and cluster head 2) to CH2(Cluster head 2)
- Cluster head 2 to server agent
- Server agent to Cluster head 1
- Cluster head 1 to destination node

The graph shows that CH1 starts monitoring at time 0sec.at time 2 sec, the nodes start transmitting. Throughput increases almost continuously from 2sec to 3.5 sec and remains constant from 3.5 to 6.5 sec and then gradually increases from 6.5 to 8sec. Throughput is increasing during the simulation that shows better network performance.

VII. Conclusion

The proposed work has reached to the conclusion that this technique is more efficient than the existing techniques in reducing packet loss, increasing throughput, and reducing jitter. The server agent technique is a centralised approach which allows trusted communication between sources and destination. The concept of cluster heads improves network efficiency. The packets are dropped whenever un trusted node comes in a way resulting, the transmitting data is not leaked out or stolen hence complete the future work described in reference paper [10].

VIII. Future Work

The simulation is done by taking 20 mobile nodes. The proposed method can be simulated for large number of nodes (say 50 or above) and then finding out the performance of the network. Also the end to end delay may be lowered at the starting of the node participation.

References

[1]. Abbas, S., Lightweight Sybil Attack Detection in MANETs, Systems Journel, IEEE (Volume:7 , Issue: 2),236-248,,2013

[2]. RoopaliGarg1, Himika Sharma2, Comparison between Sybil Attack Detection Techniques, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (Volume:3 , Issue: 2), 7142-7147,2014

[3]. Shalini.A, Arulkumaran.G, Srisathya.K.B, Taming enactment using neighbour discover distance against masquerading attack in manet, International Journal of Computer & Science (Volume:4 , Issue: 1), 1-6,,2014

[4]. P.Kavitha, C.Keerthana, V.Niroja, V.Vivekanandhan, Mobile-id Based Sybil Attack detection on the Mobile ADHOC Network, International Journal of Communication and Computer Technologies (Volume:2 ,Issue: 2), 2014

[5]. Sakil Ahmad Ansari, Mohammad Danish, An Analytical Approach on Intrusion Detection System in MANETS for Attacks, International Journal of Advanced Research in Computer Science and Software Engineering Volume:4,Issue: 3), 1058-1063, 2014

[6]. M.Praveena, R.M.Thiribhurabhavan, R.M.Bhavadharini, Dr.S.Karthik, An Enhanced Adaptive Security Protocol For Replica Attacks In Mobile Adhoc Networks, International Journal of software and hardware Research in Engg. (Volume:2,issue:5), 79-83,2014

[7]. Athira V Panicker, JIsha G, Network Layer Attacks and Protection in MANET-A Servey, IEEE Wireless Communications (Volume:5 , Issue: 3), 3437-3443,2014

[8]. Maulik H. Davda1, Sheikh R. Javid, A Review Paper on the Study of Attacks in MANET with Its Detection & Mitigation Schemes, IEEE International Journal of Advance Research in Computer Science and Management Studies (Volume:2,issue:4), 143-151,2014

[9]. Manisha, Dr. Mukesh Kumar, Network Layer Attacks and Their Countermeasures in Manet: A Review, IOSR Journal of Computer Engineering (Volume:16 , Issue: 2), 113-116, 2014

[10]. Dr. C. N. Shighe, effective algorithm for reduced packet loss in Sybil attacks, International Refereed Journal of Reviews and Research(Volume:2 , Issue: 1),2014

[11]. Keli Zhang, Zhongxian Li1, and Yixian Yang, A Reputation System Preserving the Privacy of Feedback Providers and Resisting Sybil Attacks, International Journal of Multimedia and Ubiquitous Engineering, (Volume:9,Issue:2), 141-152, 2014

[12]. Heena Sharma, Awan Dhawan, An Enhanced and efficient mechanism to detect Sybil attack in Wireless Sensor Networks, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), (Volume:2 , Issue: 2), February 2013

[13]. V. Venkata Ramana, Dr. A. Rama Mohan Reddy, and Dr. K. Chandra Sekaran, "Bio Inspired Approach to Secure Routing in MANETs", International Journal of Artificial Intelligence & Applications (IJAIA(Volume:3 , Issue: 4),July 2012

[14]. Arif Sari and Dr. Beran Necat, "Securing Mobile Ad-Hoc Networks Against Jamming Attacks Through Unified Security Mechanism", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.3, No.3, June 2012

[15]. Manoj V, Mohammed Aaqib, Raghavendiran N and Vijayan R, "A Novel Security Framework Using Trust And Fuzzy Logic In Manet", International Journal of Distributed and Parallel Systems (IJDPS) (Volume:3,Issue:1), January 2012

[16]. Gagandeep, Aashima, Pawan Kumar, Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review, (IJEAT)(Volume:1,Issue:5),June 2012.

[17]. R.Madhumathi1 & J.Jenno Richi Benat, attacks in mobile ad hoc networks: detection and counter measure, International Journal of Smart Sensors and Ad Hoc Networks(Volume:2,Issue 1), 2012

[18]. Manikandan, S.P. and R. Manimegalai, Survey on Mobile Ad Hoc Network Attacks and mitigation using routing protocols, American Journal of Applied Sciences, (Volume:9,Issue 11),1796-1801,2012

[19]. Amol Vasudeva and Manu Sood, Sybil Attack on Lowest Id Clustering Algorithm in the Mobile Ad Hoc Network, International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.5, September 2012

[20]. Shalini.A, Arulkumaran.G, Srisathya.K.B, Taming Enactment using Neighbor Discover Distance against Masquerading Attack in MANET, International Journal of Computer Engineering & Science, (Volume:4,Issue:1), Jan. 2014, 1-6, 2012.